(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－295876

(43)公開日　平成７年(1995)11月10日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/00	５３７　Ａ	7608－5B		
	12/14	３１０　Ｋ			

審査請求　未請求　請求項の数１　ＯＬ　（全　７　頁）

(21)出願番号　特願平6－81752

(22)出願日　平成６年(1994)４月20日

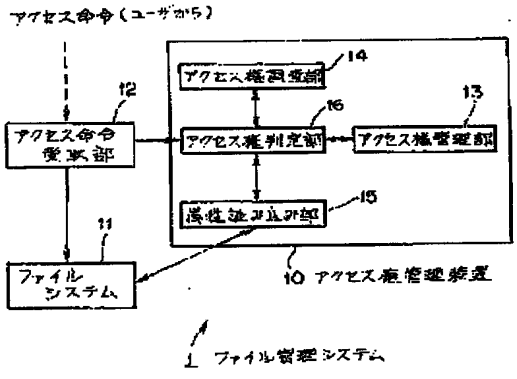
(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号

(72)発明者　長谷川　賢史
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ&Ｄ　ビジネスパークビル
富士ゼロックス株式会社内

(74)代理人　弁理士　木村　高久

(54)【発明の名称】　アクセス権管理装置

(57)【要約】
【目的】ファイルシステムの権管理装置において、アクセス権を包括的に管理できるようにする。
【構成】アクセス権判定部１６はアクセス権管理部１３で管理するファイルの属性値に関する情報と、アクセス権調査部１４で調べたアクセス権と、属性読み込み部１５で読み込んだファイルの属性値とを比較し、アクセス対象のファイルに付随する属性値やユーザのアクセス権が、アクセス権管理部１３から読み込んだファイルの属性値に関する情報に含まれるか否かを判定し、属性値やアクセス権がファイルの属性値に関する情報に含まれるときは、ファイルに対するアクセス権なしと判定し、アクセス命令受取部１２に対して、アクセス命令を発行したユーザにアクセス権がないことを通知する。



1

【特許請求の範囲】
【請求項１】　アクセス制御の対象となるファイルの属性値に関する情報を保持する属性値保持手段と、
アクセスの対象となるファイルに付随する属性値が、前記属性値保持手段で保持するファイルの属性値または属性値の範囲に含まれるか否かを判定する属性値判定手段と、
前記判定の結果を参照して、アクセスの対象となるファイルに対するアクセス権の有無を決定するアクセス権決定手段と、
を具えたことを特徴とするアクセス権管理装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】この発明は、ファイルシステムのセキュリティー管理を行うアクセス権管理装置に関する。
【０００２】なお、この明細書において、アクセスとはファイルに対する各種のオペレーション操作を含むものとする。
【０００３】
【従来の技術】従来のファイルシステムにおいて、ファイルに対するアクセス制御は、ファイル毎に設定されているアクセス権やパスワードなどの属性によって判断されていた。
【０００４】例えばＵｎｉｘでは、図１０に示すように、ファイル毎にＲｅａｄ権、Ｗｒｉｔｅ権、Ｅｘｅｃｕｔｅ権の３つのアクセス権があり、それぞれに「自分」、「自分の所属グループ」、「他人」という３つのユーザのアクセスの可否を設定できるようになっている。図１０では、ファイルの管理者（自分）には全てのアクセス権が設定され、所属グループはＲｅａｄ権のみ、他人は全てのアクセス権が制限されている。
【０００５】また、パスワードによるアクセス制御では、あらかじめファイルにパスワードを設定しておき、ファイルにアクセス要求が来た場合には、そのファイルに設定されているパスワードの入力を要求し、パスワードが正しい場合にのみアクセスを許可するようになっている。
【０００６】
【発明が解決しようとする課題】ところで、アクセス権についての情報はファイル一つ一つに設定されるため、ファイル全体のアクセスを制限したいとき、例えば「作成日時が１９９３年以降のファイルは、全ての人はアクセスできない」、あるいは「タイトルＡのファイルに対するアクセス権が全てのユーザにない」というようなアクセス制御を行うときは、ファイル一つ一つについてアクセス権の設定を行わなければならず、多くの手間と時間が必要となっていた。
【０００７】この発明は、アクセス権を包括的に管理することが可能なアクセス権管理装置を提供することを目的とする。

2

【０００８】
【課題を解決するための手段】上記課題を解決するため、この発明に係わるアクセス権管理装置は、アクセス制御の対象となるファイルの属性値に関する情報を保持する属性値保持手段と、ユーザのアクセス命令の対象となったファイルに付随する属性値が、前記属性値保持手段で保持するファイルの属性値または属性値の範囲に含まれるか否かを判定する属性値判定手段と、前記属性値判定手段での判定の結果を参照して、ファイルに対するアクセス権の有無を決定するアクセス権決定手段とを具えたことを特徴とする。
【０００９】ファイルに付随する属性値としては、例えば作成日時、作成者、タイトル名などがある。また、アクセス制御の対象となるファイルの属性値に関する情報とは、前記作成日時や作成者などの値、または値の範囲をいう。
【００１０】
【作用】ユーザからアクセス命令が発行されると、属性値判定手段はユーザのアクセス命令の対象となったファイルに付随する属性値をファイルから読み出すとともに、属性値保持手段からアクセス命令の対象となったファイルの属性値に関する情報を読み出す。そして、ユーザのアクセス命令の対象となったファイルに付随する属性値が、前記属性値保持手段から読み出したファイルの属性値または属性値の範囲に含まれるか否かを判定する。アクセス権決定手段は、前記属性値判定手段での判定の結果、ファイルに付随する属性値がファイルの属性値または属性値の範囲に含まれるときは、アクセス命令を発行したユーザはファイルへのアクセス権がない（あるいはアクセス権がある）と決定する。
【００１１】これによれば、ファイルに付随する属性値に対して、特定の値あるいは値の範囲をファイルの属性値に関する情報として設定することにより、ファイルへのアクセスを作成日時、作成者、タイトル名などの属性で制御することができるので、ファイル全体のアクセス権を包括的に管理することが可能となる。
【００１２】
【実施例】以下、この発明に係わるアクセス権管理装置を適用したファイル管理システムの一実施例を図面とともに説明する。
【００１３】図１は、この実施例におけるファイル管理システム１の機能的な構成を示すブロック図である。図において、１１はファイルシステム、１２はアクセス命令受取部、１３はアクセス権管理部、１４はアクセス権調査部、１５は属性読み込み部、１６はアクセス権判定部を表している。このうち、アクセス権管理部１３、アクセス権調査部１４、属性読み込み部１５、アクセス権判定部１６によりアクセス権管理装置１０が構成される。

【００１４】ファイルシステム１１は、ファイル管理プロセスに従って複数のファイルを管理する。ファイルシステム１１に格納されるファイルは、例えばテキストデータやイメージデータなどのファイルの内容部と、このファイルに付随する作成日時、作成者、タイトル名などのファイルの属性部により構成されている。アクセス命令を発行したユーザにアクセス権がある場合は、ユーザのアクセス命令はアクセス命令受取部１２からファイルシステム１１に渡され、その後は図示せぬオペレーション実行部を介してユーザによるファイルアクセスが行われる。

【００１５】アクセス命令受取部１２は、ユーザからファイルシステム１１へのアクセス命令を受け取り、このアクセス命令を一旦アクセス権管理装置１０に渡す。そして、アクセス権管理装置１０から、アクセス命令を発行したユーザにアクセス権があるとの決定を受け取ったときは、ユーザからのアクセス命令をファイルシステム１１に渡す。また、ユーザにアクセス権がないとの決定を受け取ったときは、ユーザからのアクセス命令をファイルシステム１１に渡さない。

【００１６】アクセス権管理部１３は、アクセス制御の対象となるファイルの属性値に関する情報として、属性を識別するための属性識別子、当該属性識別子の属性値または属性値の範囲、当該属性値または属性値の範囲に対するアクセス権、対象となるユーザ名を管理している。アクセス権管理部１３で管理しているテーブルの基本的な構成を図２に示す。テーブルを構成する各レコードは、属性識別子を表す「属性名」、これに対応する「属性値」、対象となるユーザの「ユーザ名」、否定されるアクセス権を表す「アクセス権」の項目を持っている。図２のテーブルでは、「属性名」の欄で指定された属性について、「属性値」の欄で指定された属性値を持つようなファイルに対して、「ユーザ名」の欄で指定されたユーザが「アクセス権」の欄で指定されたアクセス権を持てないことを示している。これらファイルの属性値に関する情報は、ユーザインターフェースを通じて書込み、追加、訂正、変更を行うことができる。

【００１７】アクセス権管理部１３には、少なくとも属性識別子と属性値、または属性識別子と属性値の範囲が登録されていれば、アクセス権管理装置としての機能を実現することができる。例えば、属性識別子を作成日時とし、属性値として作成年（西暦）を設定すれば、「作成日時が１９９３年以降のファイルは、全てのAはアクセスできない」というようなアクセス制御を行うことができる。

【００１８】アクセス権調査部１４は、アクセス命令受取部１２で受け取ったアクセス命令を解釈し、当該アクセス命令の実行に必要なアクセス権を検出する。検出されたアクセス権はアクセス権判定部１６に渡される。

【００１９】属性読み込み部１５は、アクセス命令の対象となったファイルに付随する属性値を、ファイルシステム１１から読み込む。前述したように、ファイルは作成日時、作成者、タイトル名などのファイルの属性部を持っているため、この属性部から必要な属性値を読み込む。読み込まれた属性値はアクセス権判定部１６に渡される。

【００２０】アクセス権判定部１６は、アクセス権管理部１３で管理するファイルの属性値に関する情報と、アクセス権調査部１４で調べたアクセス権と、属性読み込み部１５で読み込んだファイルの属性値とを比較し、アクセス対象のファイルに付随する属性値やユーザのアクセス権が、アクセス権管理部１３から読み込んだファイルの属性値に関する情報に含まれるか否かを判定する。この判定の結果、属性値やアクセス権がファイルの属性値に関する情報に含まれるときは、ファイルに対するアクセス権はないと決定し、アクセス命令受取部１２に対して、アクセス命令を発行したユーザにアクセス権がないことを通知する。また、属性値やアクセス権がファイルの属性値に関する情報に含まれないときは、ファイルに対するアクセス権があると決定し、アクセス命令を発行したユーザにアクセス権があることを通知する。

【００２１】なお、アクセス権管理部１３のテーブル（図２）の記述を変えることにより、アクセス命令に係わる属性値やアクセス権がファイルの属性値などの情報に含まれるときにはファイルに対するアクセス権があり、含まれないときにはファイルに対するアクセス権がないと決定することもできる。

【００２２】図３は、図１に示したファイル管理システム１を実現するための具体例を示したもので、ファイルサーバとして機能するコンピュータシステムのハードウェア構成を示している。

【００２３】ＣＲＴ２１はディスプレイ画面を具えたユーザインターフェースであり、画面上にテキストデータや図形などを表示する。これらの画像表示は、図示せぬＣＲＴ制御部により制御されている。

【００２４】キーボード（ＫＢ）２２はコマンドや文字列などのデータ入力用のユーザインターフェースであり、画面上で指示選択を行うための図示せぬマウスなどが接続される。キーボード２２から入力された各種のデータや指示は、図示せぬキーボード／マウス制御部を通じてプロセッサ２５に送られる。

【００２５】ディスク装置２３は磁気ディスクなどの大容量記憶装置で構成され、各種データをファイル形式で格納している。ディスク装置２３におけるデータの入出力は図示せぬディスク装置制御部により管理される。

【００２６】主メモリ２４はＲＡＭなどのメモリ装置で構成されるバッファ記憶であり、各種プログラムのほか、キーボード２２から入力された各種のデータや命令などを一時的に記憶する。プロセッサ２５が必要とするプログラムやデータは、ディスク装置２３などの２次記

憶装置から、主メモリ２４に記憶内容の一部または全部がコピーされる。

【００２７】プロセッサ２５はＣＰＵおよびその周辺回路により構成される中央処理装置であり、制御プログラムに従って上記各部の動作を管理し、また所定のデータに対する演算処理などを実行する。

【００２８】通信制御部２６は、図示せぬネットワークと接続され、ファイルシステムを利用するユーザの操作するパソコンやワークステーションなどのユーザマシンや、他のサーバとの間で行われるデータの送受信を制御する。

【００２９】図３に示すファイルサーバには、リモートにあるユーザマシンからネットワークを通じてアクセス命令が発行される。この場合、リモートのユーザマシンは少なくとも通信制御部２６の機能を具えている必要がある。なお、ファイルサーバはローカルからアクセスできることは言うまでもない。

【００３０】次に、上述したファイル管理システム１において、ユーザからファイルシステムへのアクセス命令を受け取ったときの基本的な処理の流れを図４のフローチャートにより説明する。

【００３１】アクセス命令受取部１２はユーザからファイルシステム１１へのアクセス命令を受け取ると、アクセス権管理装置１０に対して、アクセス命令を発行したユーザにアクセス権があるかどうかの判定を依頼する（ステップ１０１、ステップ１０２）。アクセス権管理装置１０では後述する図５のフローチャートに従ってアクセス権の判定を行い、判定結果をアクセス命令受取部１２に渡す（ステップ１０３）。アクセス命令受取部１２は受け取った判定結果を解釈して、アクセス命令を発行したユーザにアクセス権があるかどうかを調べる（ステップ１０４）。ユーザにアクセス権があるときはファイルシステム１１に対してアクセス命令を渡す（ステップ１０５）。また、ユーザにアクセス権がないときは、ファイルシステム１１に対してアクセス命令を渡さない（ステップ１０６）。

【００３２】なお、ユーザにアクセス権がない場合は、例えば通信制御部２６（図３）を介してユーザにエラーを返すなどの処理を行うようにしてもよい。

【００３３】次に、アクセス命令受取部１２からユーザのアクセス権があるかどうかの判定依頼があったときのアクセス権管理装置１０での処理の流れを図５のフローチャートにより説明する。

【００３４】まず、アクセス権判定部１６はアクセス権調査部１４に対して、アクセス命令受取部１２で要求されたアクセス命令の実行に必要なアクセス権の調査を依頼する。アクセス権調査部１４は依頼されたアクセス命令を解釈し、当該アクセス命令の実行に必要なアクセス権を検出する（ステップ２０１）。検出されたアクセス権はアクセス権判定部１６に渡される。アクセス権判定部１６はアクセス権管理部１３から、アクセス制御の対象となるファイルの属性値に関する情報を読み込む（ステップ２０２）。続いて、属性読み込み部１５を通じて、アクセス対象となったファイルの属性値を読み込む（ステップ２０３）。アクセス権判定部１６はアクセス権調査部１４で調べたアクセス権と、アクセス権管理部から読み込んだファイルの属性値に関する情報と、属性読み込み部で読み込んだファイルの属性値とを比較し、アクセス対象となったファイルに付随する属性値やユーザのアクセス権が、アクセス権管理部１３から読み込んだファイルの属性値に関する情報に含まれるか否かを判定する（ステップ２０４、ステップ２０５）。ここで、アクセス対象のファイルに付随する属性値やユーザのアクセス権がファイルの属性値に関する情報に含まれるときは、ユーザにアクセス権なしと決定し、アクセス命令受取部１２に対して、ユーザにアクセス権がないことを通知する（ステップ２０６）。また、アクセス対象のファイルに付随する属性値やユーザのアクセス権がファイルの属性値に関する情報に含まれないときは、ユーザにアクセス権ありと決定し、アクセス命令受取部１２に対して、ユーザにアクセス権があることを通知する（ステップ２０７）。

【００３５】図６～図８は、アクセス権管理部１３で管理しているテーブルの一例を示している。次に、上述したアクセス権判定部１６において、アクセス対象のファイルに付随する属性値やユーザのアクセス権がファイルの属性値に関する情報に含まれるか否かを判定する処理の具体例を図６のテーブル例とともに説明する。

【００３６】図６に示すテーブルは、ファイルを作成した日時を制御対象（属性値）としたもので、作成日時を格納する属性である「ＣｒｅａｔｅＤａｔｅＡｎｄＴｉｍｅ」によってアクセスの制御を行っている。また、属性値は最大値（期間の最初）と最小値（期間の最後）からなる時間的な範囲で表されている。このテーブルには、次のような内容が設定されている。

【００３７】「１９９２年１月１日０時０分０秒から、１９９３年１月１日０時０分０秒の間に作成されたファイルに対するＲｅａｄ権がユーザＡにはない」

「１９８９年１０月１０日０時０分０秒から、１９９０年１０月１０日０時０分０秒の間に作成されたファイルに対するＲｅａｄ権がユーザＢにはない」

テーブル上にこのような情報が保持されている状態で、ユーザＡから１９９２年１０月１０日に作成されたファイルに対するＲｅａｄのアクセス命令が発行された場合について考えてみる。

【００３８】まず、アクセス権調査部１４ではアクセス権判定部１６から依頼されたアクセス命令を解釈し、当該アクセス命令の実行に必要なアクセス権を検出する。この結果、Ｒｅａｄ（権）が得られる。次に、アクセス権判定部１６はアクセス権管理部１３から、図６のよう

なアクセス制御の対象となるファイルの属性値に関する情報を読み込む。続いて、アクセス権判定部16は属性読み込み部15から、アクセス対象となったファイルの属性値（この例では作成日時）を読み込む。これにより、ユーザAのアクセス権を判定するための条件が揃ったことになる。

【0039】ここで、ファイルに付随する属性値やユーザのアクセス権が、アクセス権管理部13から読み込んだファイルの属性値に関する情報に含まれるか否かを判定する場合の処理の流れを図9のフローチャートにより説明する。

【0040】最初に、アクセス命令を発行したユーザ名と一致するユーザ名がテーブル上に存在するかどうかを調べる（ステップ301）。ユーザAと一致する名前は、図5の先頭のレコードのユーザ名の項目にある。次に、先頭のレコードについて、アクセス命令の実行に必要なアクセス権と一致するアクセス権が存在するかどうかを調べる（ステップ302）。アクセス命令の実行に必要なアクセス権と一致するReadは、当該レコードのアクセス権の項目にある。続いて、アクセス対象ファイルの作成日時が、ファイルの属性値の範囲に含まれるかどうかを調べる（ステップ303）。ファイルの作成日時である1992年10月10日は、ファイルの属性値の範囲「1992年1月1日0時0分0秒から1993年1月1日0時0分0秒」の間に含まれる（ステップ303「Y」）。したがって、アクセス権判定部16は、アクセス命令を発行したユーザはアクセス権を持っていないと判定する（ステップ304）。なお、ステップ301～ステップ303で一致する条件が一つでもないときは、アクセス命令を発行したユーザはアクセス権を持っているものと判定する（ステップ305）。

【0041】なお、図9のフローチャートは判定処理の基本的な流れを説明するためのもので、実際の判定処理の手順を示したものではない。

【0042】図6の例のように、「CreateDateAndTime」によるアクセス制御は、例えば「1993年以降に作成されたファイルには最新のデータが入っているため公開するべきではないので、特定の人以外はReadできないようにする。」というような制御を行う場合に便利である。

【0043】図7に示すテーブルは、ファイルを最後に変更したユーザ名を属性値としたもので、最終更新者名を格納する属性である「LastModifiedBy」によってアクセスの制御を行っている。このテーブルには、次のような内容が設定されている。

【0044】「ユーザAが最後に修正したファイルに対するWrite権がユーザA以外の人にはない」

「ユーザBが最後に修正したファイルに対するRead権がユーザB以外の人にはない」

図7の例のように、「LastModifiedBy」によるアクセス制御は、例えば「Aという人は最終的にファイルの内容をチェックする人なので、この人がチェックをして内容を変更した後は、その他の人は変更してはいけない。」という場合や、「Bという人はファイルの内容に関して評価して機密事項を書き込むので、この人がチェックをして内容を変更した後は、その他の人はこのファイルを見ることができない。」というような制御を行う場合に便利である。

【0045】図8に示すテーブルは、ファイルのタイトル名を属性値としたもので、タイトル名を格納する属性である「Title」によってアクセスの制御を行っている。このテーブルには、次のような内容が設定されている。

【0046】「タイトルが「極秘＊」（＊は任意の文字列）であるファイルに対する全てのアクセス権が、全ての人にない。」

「タイトルが「＊（Aonly）」（例：「技術データ（Aonly）」）であるファイルに対する全てのアクセス権が、A以外の人にない。」

図8の例のように、「Title」によるアクセス制御は、ファイル名の意味によりアクセス権を制御する場合に便利である。また、属性値としては、ディレクトリで用いられる、／A／B／C、／A／B／Dというようなパス名を使用してもよい。

【0047】図7や図8のアクセス制御においても、アクセス対象となったファイルに付随する属性値やユーザのアクセス権が、アクセス権管理部13から読み込んだファイルの属性値に関する情報に含まれるか否かを判定する場合の処理手順は、図9に準じたフローチャートにより実現することができる。

【0048】上述した実施例では、ファイルに付随する作成日時、作成者、タイトル名などの属性値をアクセス権の判定に使用しているが、これらの属性値は一つだけでなく、他の属性値と組み合わせて設定してもよい。また、ファイルに特別な属性値を付加し、この属性値をアクセス権の判定に使用することもできる。

【0049】

【発明の効果】以上説明したように、この発明に係わるアクセス権管理装置では、アクセス制御の対象となるファイルの属性値に関する情報を保持し、ユーザのアクセス命令の対象となったファイルに付随する属性値が、前記保持するファイルの属性値または属性値の範囲に含まれるか否かによって、ファイルに対するアクセス権の有無を決定するようにしたため、ファイルに付随する作成日時や作成者、タイトル名などの属性値を操作することにより、ファイル全体のアクセス権を包括的に管理することが可能となる。

【図面の簡単な説明】

【図1】ファイル管理システムの機能的な構成を示すブロック図。

9

【図２】アクセス権管理部で管理しているテーブルの基本的な構成を示す図

【図３】コンピュータシステムのハードウェア構成を示す図

【図４】ファイル管理システムの処理の流れを示すフローチャート

【図５】アクセス権管理装置の処理の流れを示すフローチャート

【図６】作成日時を属性値とするテーブルの一例を示す図

【図７】作成者を属性値とするテーブルの一例を示す図＊

10

＊【図８】タイトル名を属性値とするテーブルの一例を示す図

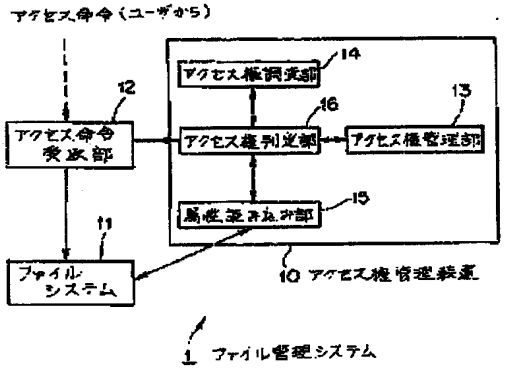
【図９】アクセス権判定部の処理の流れを示すフローチャート

【図１０】アクセス権と対象ユーザの関係を示す図

【符号の説明】

１…ファイル管理システム、１０…アクセス権管理装置、１１…ファイルシステム、１２…アクセス命令受付部、１３…アクセス権管理部、１４…アクセス権調査部、１５…属性読み込み部、１６…アクセス権判定部

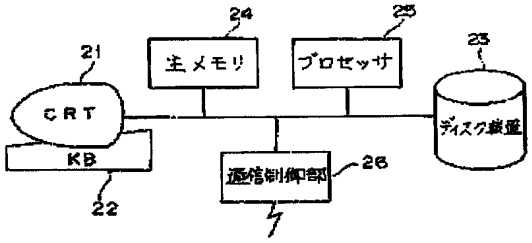
【図１】



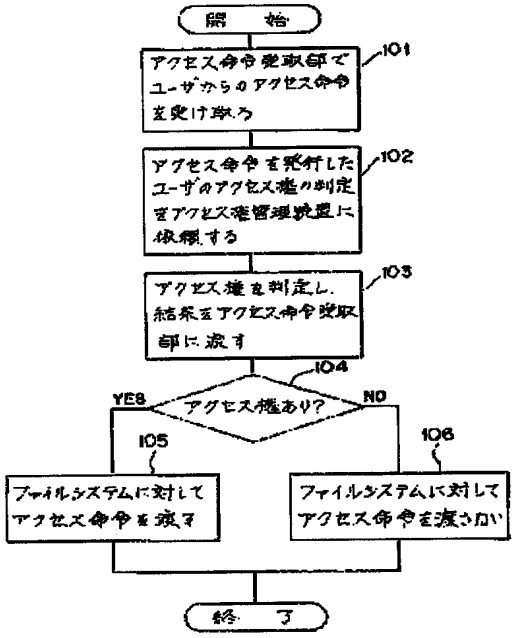
【図２】

属性名	属性値	ユーザ名	アクセス権
○○○	△△	□□□	×××

【図３】



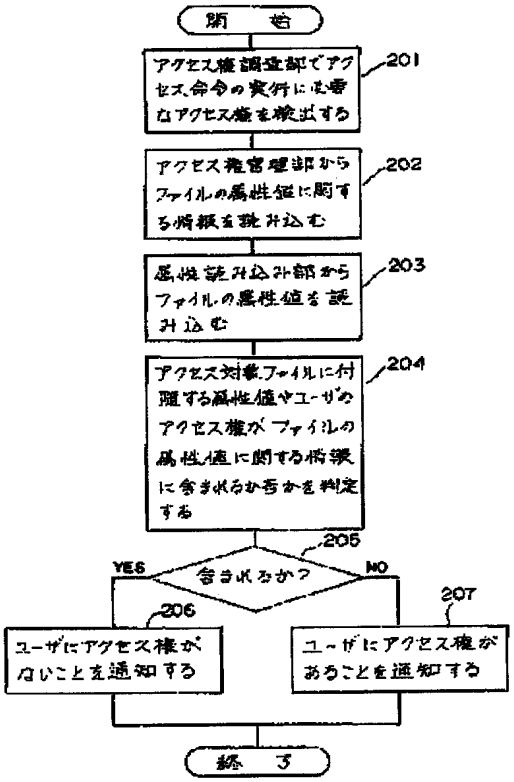
【図４】



【図７】

属性名	属性値	ユーザ名	アクセス権
LastModifiedBy	A	Not A	Write
LastModifiedBy	B	Not B	Read

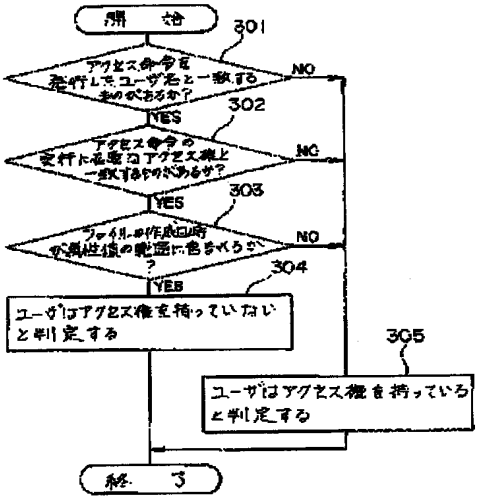
【図5】



【図6】

属性名	属性値		ユーザ名	アクセス権
	最大値	最小値		
CreateDateAndTime	1992 1/1 0:0:0	1996 1/1 0:0:0	A	Read
CreateDateAndTime	19991010:0:0:0	19901010 0:0:0	B	Read

【図9】



【図8】

属性名	属性値	ユーザ名	アクセス種
Title	修飾*	ALL	ALL
Title	*(Anony)	Not A	ALL

【図10】

	Read	Write	Exe,
自分	○	○	○
グループ	○	×	×
他人	×	×	×

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-295876
(43)Date of publication of application : 10.11.1995

(51)Int.Cl. G06F 12/00
G06F 12/14

(21)Application number : 06-081752
(22)Date of filing : 20.04.1994

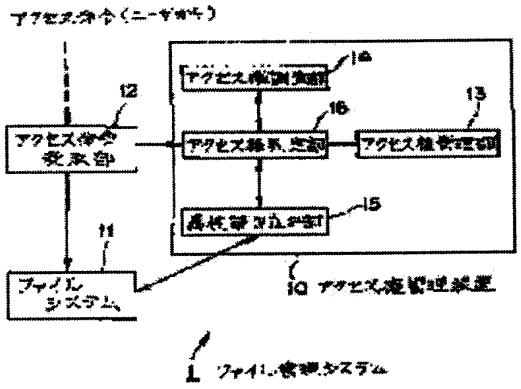
(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : HASEGAWA MASASHI

(54) ACCESS RIGHT CONTROLLING DEVICE

(57)Abstract:

PURPOSE: To comprehensively control an access right in the access right controlling device of a file system.

CONSTITUTION: An access right judging part 16 compares information related to the attribute value of a file controlled by an access right control part 13, the access right investigated by an access right investigating part 14 with the attribute value of the file read by an attribute reading part 15, and judges whether or not the attribute value appendant to the object file to be accessed or the access right of a user is included in the information related to the attribute value of the file read from the access right control part 13, and when the attribute value or the access right is included in the information related to the attribute value, it is judged that there is no access right for the file, and the part 16 informs an access instruction receiving part 12 of that the user having issued an access instruction has no access right.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The access privilege management equipment carry out having had an attribute-value judging means judge whether the attribute value which accompanies the file set as an attribute-value maintenance means hold the information about the attribute value of a file set as the object of an access control, and the object of access is included in the range of the attribute value of the file which holds with said attribute-value maintenance means, or attribute value, and an access privilege decision means determine the existence of the access privilege to the file from which it is set as the object of access with reference to the result of said judgment as the description.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the access privilege management equipment which performs security management of a file system.
[0002] In addition, in this description, various kinds of operation actuation to a file shall be included with access.
[0003]
[Description of the Prior Art] In the conventional file system, the access control to a file was judged with the attribute of the access privilege set up for every file, a password, etc.
[0004] For example, in Unix, as shown in drawing 10 , there are three access privileges, a Read right, a Write right, and an Execute right, for every file, and the propriety of access of the three users "itself", "its affiliation group", and "others" can be set now as each. In drawing 10 , all access privileges are assigned to the manager (themselves) of a file, and, as for the affiliation group, all access privileges are restricted only for the Read right, as for others.
[0005] Moreover, in an access control with a password, when the password is beforehand set as the file and an access request comes to a file, the input of the password set as the file is required, and a password permits access only to a right case.
[0006]
[Problem(s) to be Solved by the Invention] Since the information about an access privilege is set as file each, "date and time of creation to restrict access of the whole file by the way, the file in 1993 and afterwards When performing that no men can access" or the access control "not all users have an access privilege to the file of Title A", the access privilege had to be set up about file each and much time and effort and time amount were needed.
[0007] This invention aims at offering the access privilege management equipment which can manage an access privilege comprehensively.
[0008]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the access privilege management equipment concerning this invention An attribute value maintenance means to hold the information about the attribute value of a file set as the object of an access control, An attribute value judging means to judge whether the attribute value which accompanies the file set as the object of an access instruction of a user is included in the range of the attribute value of the file held with said attribute value maintenance means, or attribute value, It is characterized by having an access privilege decision means to determine the existence of the access privilege to a file, with reference to the result of a judgment with said attribute value judging means.
[0009] As attribute value which accompanies a file, there are the date and time of creation, an implementer, a title name, etc., for example. Moreover, the information about the attribute value of a file set as the object of an access control says the range of the value of said date and time of creation, implementer, etc., or a value.

[0010]
[Function] If an access instruction is published from a user, an attribute value judging means will read the information about the attribute value of a file set from the attribute value maintenance means as the object of an access instruction while reading from a file the attribute value which accompanies the file set as the object of an access instruction of a user. And it judges whether the attribute value which accompanies the file set as the object of an access instruction of a user is included in the range of the attribute value of the file read from said attribute value maintenance means, or attribute value. The user who, as for the access privilege decision means, published the access instruction when the attribute value which accompanies a file was included in the range of the attribute value of a file or attribute value as a result of a judgment with said attribute value judging means determines that there is no access privilege to a file (or there is an access privilege).
[0011] Since access to a file is controllable by attributes, such as the date and time of creation, an implementer, and a title name, to the attribute value which accompanies a file by setting up the range of a specific value or a value as information about the attribute value of a file according to this, it becomes possible to manage the access privilege of the whole file comprehensively.
[0012]
[Example] Hereafter, one example of the file management system which applied the access privilege management equipment concerning this invention is explained with a drawing.
[0013] Drawing 1 is the block diagram showing the functional configuration of the file management system 1 in this example. drawing -- setting -- 11 -- in the access privilege Management Department and 14, the access privilege Research and Planning Department and 15 express the attribute reading section, and 16 expresses [a file system and 12 / the access instruction receipt section and 13] the access privilege judging section. Among these, access privilege management equipment 10 is constituted by the access privilege Management Department 13, the access privilege Research and Planning Department 14, the attribute reading section 15, and the access privilege judging section 16.
[0014] A file system 11 manages multiple files according to a file management process. The file stored in a file system 11 is constituted by the content block of files, such as text data and an image data, and the attribute section of files, such as the date and time of creation which accompanies this file, an implementer, and a title name. When the user who published the access instruction has an access privilege, an access instruction of a user is passed to a file system 11 from the access instruction receipt section 12, and the file access by the user is performed through the operation activation section which is not illustrated after that.
[0015] The access instruction receipt section 12 passes the access instruction to a file system 11 from a user to reception, and once passes this access instruction to access privilege management equipment 10. And when decision that the user who published the access instruction has an access privilege is received from access privilege management equipment 10, the access instruction from a user is passed to a file system 11. Moreover, when decision that a user does not have an access privilege is received, the access instruction from a user is not passed to a file system 11.
[0016] The access privilege Management Department 13 has managed the access privilege and the target user name to the range of the range of the attribute value of the attribute identifier for identifying an attribute, and the attribute identifier concerned, or attribute value, the attribute value concerned, or attribute value as information about the attribute value of a file set as the object of an access control. The fundamental configuration of the table managed at the access privilege Management Department 13 is shown in drawing 2 . Each record which constitutes a table has the "attribute name" showing an attribute identifier, the "attribute value" corresponding to this, the target user's "user name", and the item of the "access privilege" showing the access privilege denied. On the table of drawing 2 , the user specified in the column of a "user name" to a file which has the attribute value specified in the column of "attribute value" about the attribute specified in the column of a "attribute name" shows that it cannot have the access privilege specified in the column of an "access privilege." Through a user interface, writing, an addition, and correction are performed and the information about the attribute value of these files can make a change.

[0017] The access privilege Management Department 13 can realize the function as access privilege management equipment, if the range of an attribute identifier, attribute value, or an attribute identifier and attribute value is registered at least. For example, if an attribute identifier is made into the date and time of creation and a creation year (A.D.) is set up as attribute value, the access control "the date and time of creation can access the file in 1993 and afterwards, as for [no] people" can be performed.
[0018] The access privilege Research and Planning Department 14 interprets the access instruction received in the access instruction receipt section 12, and detects an access privilege required for activation of the access instruction concerned. The detected access privilege is passed to the access privilege judging section 16.
[0019] The attribute reading section 15 reads the attribute value which accompanies the file set as the object of an access instruction from a file system 11. As mentioned above, since the file has the attribute section of files, such as the date and time of creation, an implementer, and a title name, it reads required attribute value from this attribute section. The read attribute value is passed to the access privilege judging section 16.
[0020] The access privilege judging section 16 compares the information about the attribute value of the file managed at the access privilege Management Department 13, and the access privilege investigated in the access privilege Research and Planning Department 14 with the attribute value of the file read in the attribute reading section 15, and it judges whether the access privilege of the attribute value which accompanies the file for access, or a user is contained in the information about the attribute value of the file read from the access privilege Management Department 13. When attribute value and an access privilege are contained in the information about the attribute value of a file as a result of this judgment, it determines that there is no access privilege to a file, and the user who published the access instruction is notified of there being no access privilege to the access instruction receipt section 12. Moreover, when neither attribute value nor an access privilege is contained in the information about the attribute value of a file, it determines that there is an access privilege to a file, and the user who published the access instruction is notified of there being an access privilege.
[0021] In addition, by changing description of the table (drawing 2) of the access privilege Management Department 13, when the attribute value and the access privilege concerning an access instruction are contained in information, such as attribute value of a file, there is an access privilege to a file, and when not contained, it can also be determined that there is no access privilege to a file.
[0022] Drawing 3 is what showed the example for realizing file management system 1 shown in drawing 1 , and shows the hardware configuration of the computer system which functions as a file server.
[0023] CRT21 is the user interface equipped with the display screen, and displays text data, a graphic form, etc. on a screen. Such image display is controlled by the CRT control section which is not illustrated.
[0024] A keyboard (KB) 22 is a user interface for data inputs, such as a command and a character string, and the mouse which is not illustrated for performing directions selection on a screen is connected. Various kinds of data inputted from the keyboard 22 and directions are sent to a processor 25 through the keyboard / mouse control section which is not illustrated.
[0025] A disk unit 23 consists of large capacity storage, such as a magnetic disk, and stores various data by file format. I/O of the data in a disk unit 23 is managed by the disk unit control section which is not illustrated.
[0026] Main memory 24 is a buffer store which consists of memory apparatus, such as RAM, and memorizes temporarily various kinds of data, an instruction, etc. which were inputted from the keyboard 22 besides various programs. As for the program and data which a processor 25 needs, a part or all of the content of storage is copied to main memory 24 from secondary storage, such as a disk unit 23.
[0027] A processor 25 is a central processing unit constituted by CPU and its circumference circuit, manages actuation of each part of the above according to a control program, and performs data processing to predetermined data etc.
[0028] It connects with the network which is not illustrated and the communications control section 26 controls the transmission and reception of data performed between user machines which the user using a

file system operates, such as a personal computer and a workstation, and other servers.
[0029] An access instruction is published through a network by the file server shown in drawing 3 from a remote ****** user machine. In this case, the user machine of RIMOTO needs to be equipped with the function of the communications control section 26 at least. In addition, it cannot be overemphasized that a file server can be accessed from a local.
[0030] Next, in the file management system 1 mentioned above, the flow chart of drawing 4 explains the flow of the fundamental processing when receiving the access instruction to a file system from a user.
[0031] The access instruction receipt section 12 will request the judgment of whether there is any access privilege from the user who published the access instruction to access privilege management equipment 10, if the access instruction to a file system 11 from a user is received (step 101, step 102). With access privilege management equipment 10, an access privilege is judged according to the flow chart of drawing 5 mentioned later, and a judgment result is passed to the access instruction receipt section 12 (step 103). It investigates whether the access instruction receipt section 12 interprets the received judgment result, and the user who published the access instruction has an access privilege (step 104). When a user has an access privilege, an access instruction is passed to a file system 11 (step 105). Moreover, when a user does not have an access privilege, an access instruction is not passed to a file system 11 (step 106).
[0032] In addition, when a user does not have an access privilege, it may be made to process returning an error to a user through the communications control section 26 (drawing 3) etc.
[0033] Next, the flow chart of drawing 5 explains the flow of processing with access privilege management equipment 10 when there is a judgment request whether there is any access privilege of a user from the access instruction receipt section 12.
[0034] First, the access privilege judging section 16 requests examination of an access privilege required for activation of the access instruction demanded in the access instruction receipt section 12 to the access privilege Research and Planning Department 14. The access privilege Research and Planning Department 14 interprets the requested access instruction, and detects an access privilege required for activation of the access instruction concerned (step 201). The detected access privilege is passed to the access privilege judging section 16. The access privilege judging section 16 reads the information about the attribute value of a file set as the object of an access control from the access privilege Management Department 13 (step 202). Then, the attribute value of a file used as the object for access is read through the attribute reading section 15 (step 203). The access privilege judging section 16 compares the information about the attribute value of the access privilege investigated in the access privilege Research and Planning Department 14, and the file read from the access privilege Management Department with the attribute value of the file read in the attribute reading section, and it judges whether the access privilege of the attribute value which accompanies the file used as the object for access, or a user is contained in the information about the attribute value of the file read from the access privilege Management Department 13 (step 204, step 205). Here, when the access privilege of the attribute value which accompanies the file for access, or a user is contained in the information about the attribute value of a file, it determines to have no access privilege at a user, and a user is notified of there being no access privilege to the access instruction receipt section 12 (step 206). Moreover, when the access privilege of the attribute value which accompanies the file for access, or a user is not contained in the information about the attribute value of a file, it is decided at a user that they will be those with an access privilege, and it notifies that a user has an access privilege to the access instruction receipt section 12 (step 207).
[0035] Drawing 6 - drawing 8 show an example of the table managed at the access privilege Management Department 13. Next, in the access privilege judging section 16 mentioned above, the example of processing in which the access privilege of the attribute value which accompanies the file for access, or a user judges whether it is contained in the information about the attribute value of a file is explained with the example of a table of drawing 6 .
[0036] The table shown in drawing 6 is what made time which created the file the controlled system (attribute value), and is controlling access by "CreateDateAndTime" which is the attribute which stores

the date and time of creation. Moreover, attribute value is expressed in the time range which consists of maximum (beginning of a period), and the minimum value (the last of a period). The following contents are set to this table.
[0037] "User A does not have a Read right to the file created in 0 minute and 0 second from 0:0 0 second on January 1, 1992 at 0:00 on January 1, 1993."
"User B does not have a Read right to the file created in 0 minute and 0 second from 0:0 0 second on October 10, 1989 at 0:00 on October 10, 1990."
The case where the access instruction of Read to the file created from User A on October 10, 1992 is published in the condition that such information is held on the table is considered.
[0038] First, in the access privilege Research and Planning Department 14, the access instruction requested from the access privilege judging section 16 is interpreted, and an access privilege required for activation of the access instruction concerned is detected. Consequently, Read (**) is obtained. Next, the access privilege judging section 16 reads the information about the attribute value of a file set from the access privilege Management Department 13 as the object of an access control like drawing 6 . Then, the access privilege judging section 16 reads the attribute value (this example date and time of creation) of a file used as the object for access from the attribute reading section 15. It means meeting the conditions for judging User's A access privilege by this.
[0039] Here, the access privilege of the attribute value which accompanies a file, or a user explains the flow of processing in the case of judging whether it is contained in the information about the attribute value of the file read from the access privilege Management Department 13 with the flow chart of drawing 9 .
[0040] It investigates whether first, the user name which published the access instruction, and a user name in agreement exist on a table (step 301). The identifier which is in agreement with User A is in the item of the user name of the record of the head of drawing 5 . Next, it investigates whether an access privilege required for activation of an access instruction and an access privilege in agreement exist about a top record (step 302). Read which is in agreement with an access privilege required for activation of an access instruction is in the item of the access privilege of the record concerned. Then, the date and time of creation of the file for access investigates whether it is contained in the range of the attribute value of a file (step 303). October 10, 1992 which is the date and time of creation of a file is contained between the range of the attribute value of a file "0:0 0 second on January 1, 1992 to 0:0 0 second on January 1, 1993" (step 303 "Y"). Therefore, the access privilege judging section 16 judges with the user who published the access instruction not having an access privilege (step 304). In addition, when the number of the conditions which are in agreement at step 301 - step 303 is not one, either, the user who published the access instruction judges with a thing with an access privilege (step 305).
[0041] In addition, the flow chart of drawing 9 is for explaining the fundamental flow of judgment processing, and is not what showed the procedure of actual judgment processing.
[0042] Like the example of drawing 6 , the access control by "CreateDateAndTime" is convenient, when performing control of "preventing from Read(ing) except a specific man since close requires the newest data for the file created in 1993 and afterwards and it should not open to the public."
[0043] The table shown in drawing 7 is what made attribute value the user name which changed the file at the end, and is controlling access by "LastModifiedBy" which is the attribute which stores the last regenerator name. The following contents are set to this table.
[0044] "Men other than User A do not have a Write right to the file which User A corrected at the end."
"Men other than User B do not have a Read right to the file which User B corrected at the end."
The access control by "LastModifiedBy" like the example of drawing 7 For example, other men must not change, after this man's checking and changing the content, since the men "A are those who check the content of the file eventually. since the case where it is called ", and the man "B evaluate about the content of the file and a secret matter is written in, after this man's checking and changing the content, other men cannot see this file. It is convenient when performing control, such as ".
[0045] The table shown in drawing 8 is what made the title name of a file attribute value, and is controlling access by "Title" which is the attribute which stores a title name. The following contents are

set to this table.
[0046] "Not all men have all the access privileges to the file whose title is "strictly confidential *" (* is the character string of arbitration)."
"Men other than A do not have all the access privileges to the file whose title is "*(Aonly)" (example : "an engineering data (Aonly)")."
Like the example of drawing 8 , the access control by "Title" is convenient, when controlling an access privilege by semantics of a file name. Moreover, as attribute value, /A/B/C used by the directory and a pathname, such as /A/B/D, may be used.
[0047] Also in the access control of drawing 7 or drawing 8 , the procedure in the case of judging whether the access privilege of the attribute value which accompanies the file used as the object for access, or a user is contained in the information about the attribute value of the file read from the access privilege Management Department 13 is realizable with the flow chart according to drawing 9 .
[0048] Although attribute value, such as the date and time of creation which accompanies a file, an implementer, and a title name, is used for the judgment of an access privilege in the example mentioned above, such attribute value may be set up not only combining one but combining other attribute value. Moreover, attribute value special to a file can be added and this attribute value can also be used for the judgment of an access privilege.
[0049]
[Effect of the Invention] As explained above, with the access privilege management equipment concerning this invention The attribute value which accompanies the file which held the information about the attribute value of a file set as the object of an access control, and was set as the object of an access instruction of a user by whether it is contained in the range of the attribute value of said file to hold, or attribute value Since the existence of the access privilege to a file was determined, it becomes possible to manage the access privilege of the whole file comprehensively by operating attribute value, such as the date and time of creation which accompanies a file, and an implementer, a title name.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram showing the functional configuration of file management system.
[Drawing 2] Drawing showing the fundamental configuration of the table managed at the access privilege Management Department
[Drawing 3] Drawing showing the hardware configuration of a computer system
[Drawing 4] The flow chart which shows the flow of processing of file management system
[Drawing 5] The flow chart which shows the flow of processing of access privilege management equipment
[Drawing 6] Drawing showing an example of the table which makes the date and time of creation attribute value
[Drawing 7] Drawing showing an example of the table which makes an implementer attribute value
[Drawing 8] Drawing showing an example of the table which makes a title name attribute value
[Drawing 9] The flow chart which shows the flow of processing of the access privilege judging section
[Drawing 10] Drawing showing the relation between an access privilege and a candidate user
[Description of Notations]
1 [-- The access instruction reception section, 13 / -- The access privilege Management Department, 14 / -- The access privilege Research and Planning Department, 15 / -- The attribute reading section, 16 / -- Access privilege judging section] -- File management system, 10 -- Access privilege management equipment, 11 -- A file system, 12

[Translation done.]

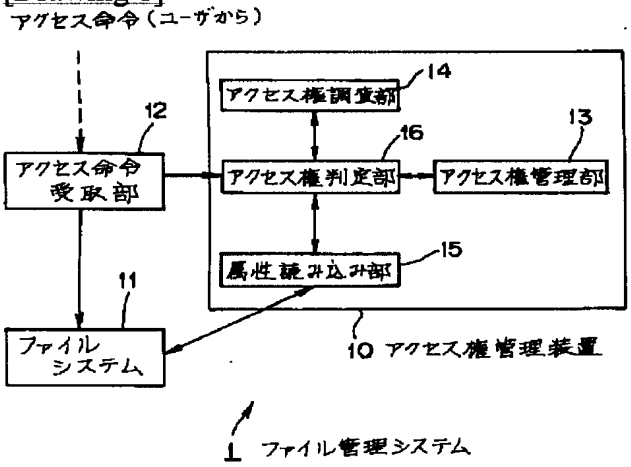
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

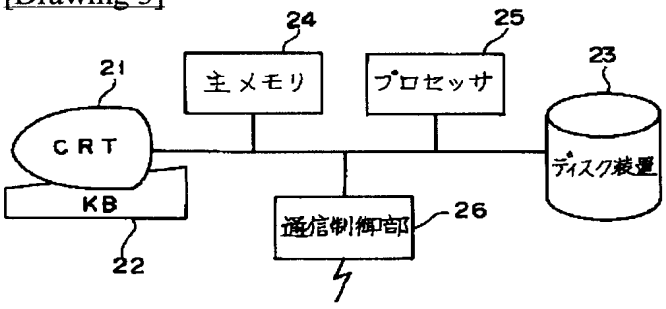
[Drawing 1]



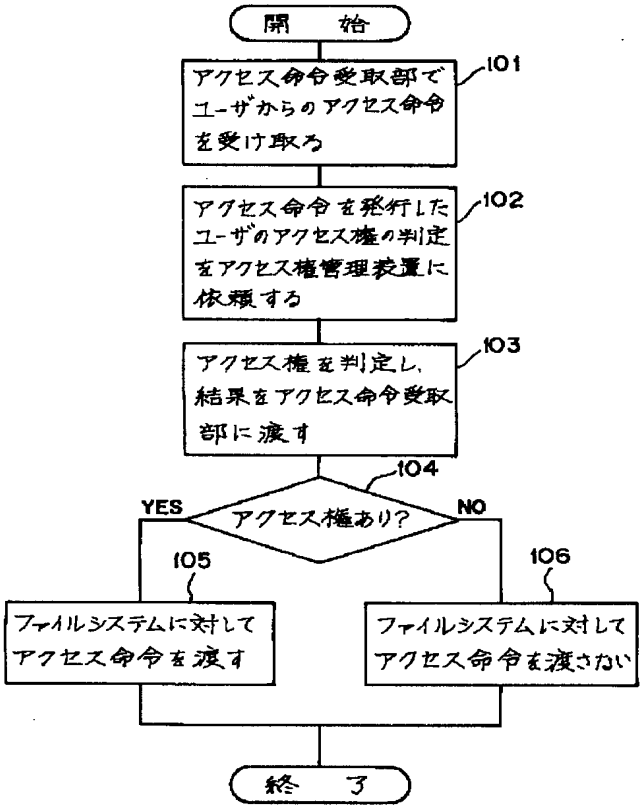
[Drawing 2]

属性名	属性値	ユーザ名	アクセス権
○○○	△△	□□□	×××

[Drawing 3]



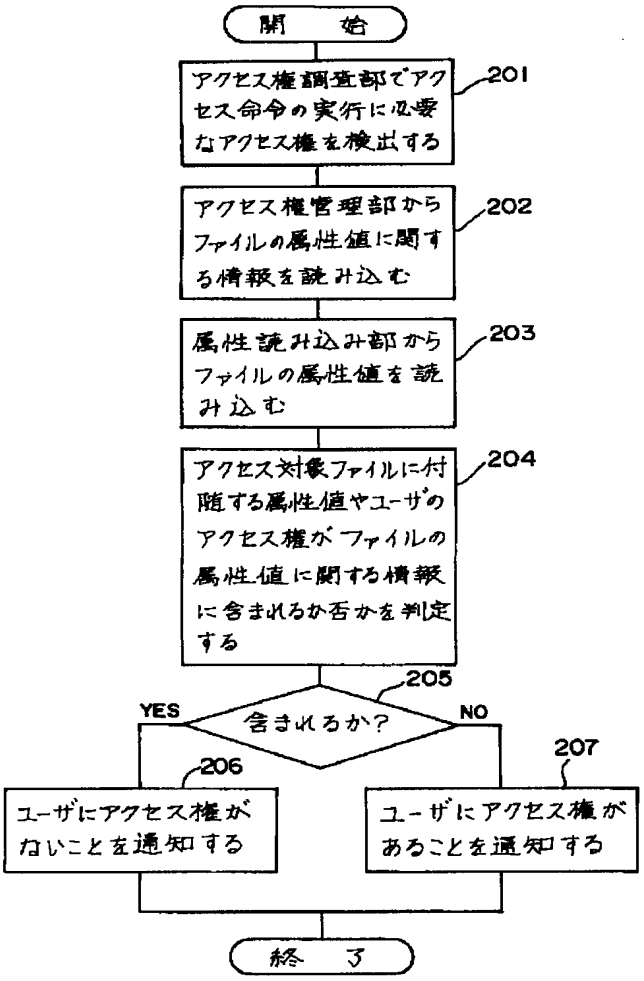
[Drawing 4]



[Drawing 7]

属性名	属性値	ユーザ名	アクセス権
LastModifiedBy	A	Not A	Write
LastModifiedBy	B	Not B	Read

[Drawing 5]



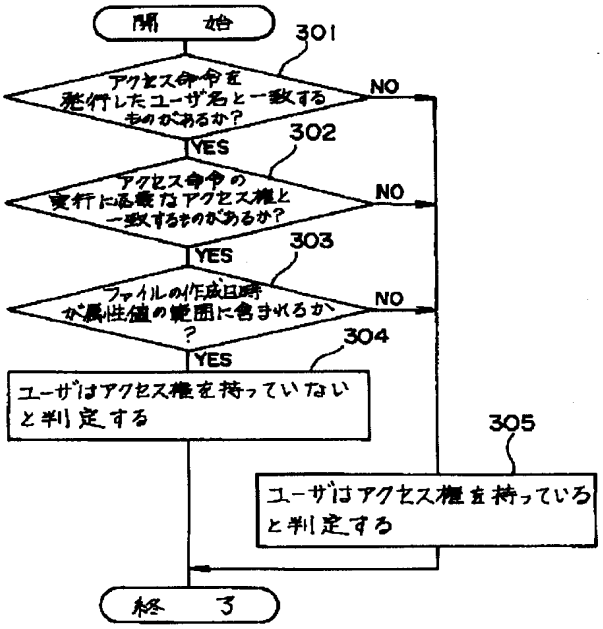
[Drawing 6]

属性名	属性値		ユーザ名	アクセス権
	最大値	最小値		
CreateDateAndTime	1992 1/1 0:0:0	1993 1/1 0:0:0	A	Read
CreateDateAndTime	19991010 0:0:0	19901010 0:0:0	B	Read

[Drawing 8]

属性名	属性値	ユーザ名	アクセス権
Title	極秘*	ALL	ALL
Title	*(Aonly)	Not A	ALL

[Drawing 9]



[Drawing 10]

	Read	Write	Exe,
自分	○	○	○
グループ	○	×	×
他人	×	×	×

[Translation done.]